

ADVANCED
WINDOWS

Working with automatic updates

Say goodbye to PC maintenance by getting your computer to update and repair itself. Peter Wood explains how to use Windows' automatic updates and third-party alternatives

Windows XP and Windows Vista both have their own automatic update features. Most security programs, and some other applications, now have a similar feature. Take a little time to learn how these features work and the update process can be made to run in the background, almost without you having to be aware of it. We say almost, because you cannot afford to be complacent about your PC's security. All automated update features are not equal, and before relying on a program to keep itself healthy it's worth doing some research and taking a few elementary precautions.

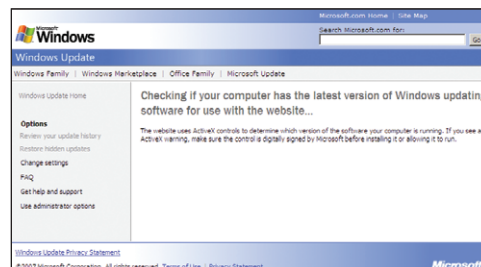
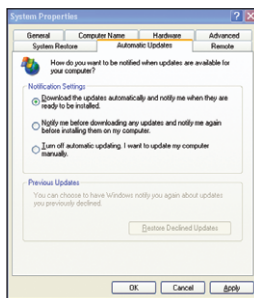
WINDOWS AUTOMATIC UPDATES

The Automatic Updates feature was first introduced with Windows 98. At that time, the program was a free download that users could choose to install or not. In Windows XP and Windows Vista, Automatic Updates is built into the operating system, although you can still choose to disable it.

If you haven't yet installed XP Service Pack 2 and you want to make sure Windows Updates is enabled, right-click My Computer and choose Properties. This will open the System Properties overview. On the Automatic Updates tab, make sure Windows is configured to download and install updates automatically. Users who have installed Service Pack 2 can configure Automatic Updates in the same way, although the interface looks a little different. Alternatively, they can use the Automatic Updates entry in the Windows Control Panel.

If you're running Windows XP Service Pack 1, you'll be able to specify only whether or not Automatic Updates is turned on, and whether it should warn you before it installs something. If you have installed Service

► Choose to have Windows notify you every time it installs an update and you may quickly tire of its nagging questions. It's far better to allow Windows to install updates automatically



▲ Using the Windows Updates website gives you access to the same software that you get through Windows XP's built-in Automatic Updates feature

Pack 2 you can also specify how often, and at what time of day, Automatic Updates should run.

Once it's enabled, Automatic Updates will periodically check the Windows Update website. If there are crucial updates available that haven't yet been installed, it will download and install them for you. It manages to do this without hogging your internet connection by using a technology called Background Intelligent Transfer Service (BITS). Before it starts downloading a file, the BITS program first checks to see what other programs are using the internet and then uses just the remainder of your bandwidth. If another program needs more bandwidth, the BITS program will automatically use less.

Windows Automatic Updates will only download updates that are vital to your PC's health and security. However, Microsoft also releases lots of other free updates to its programs that add new features that you may find useful. So from time to time, it pays to check what updates are available manually. To do this, visit either <http://windowsupdate.microsoft.com> or <http://update.microsoft.com/microsoftupdate>. The first site only updates Windows, while the second also updates other Microsoft programs such as Office. On either site, to see a list of non-critical updates simply click the button marked Custom. The website then runs an ActiveX control that examines your PC to see what updates are available for your software. You need Internet Explorer 5 or later to use this feature. Microsoft Office also has its own automatic update website (<http://office.microsoft.com/officeupdate>).

Once it has finished installing an update, Windows will nag you at regular intervals to restart your PC. To

INTRODUCTION

With new viruses and other malware detected daily, keeping your anti-virus software up to date is vital. Failure to do so increases greatly the chances of your PC being infected. Your anti-virus program is not the only thing that needs keeping up to date, however. Your firewall, your anti-spyware program, Windows itself and even your Office software all need to be updated regularly.

Making sure all the latest patches and fixes are installed on your computer will protect you against internet-borne threats and often adds new and useful features to your software. In this month's *Advanced Windows*, we show you how to protect your PC with automatic updates, and how to keep it running smoothly by scheduling important maintenance programs to run at regular intervals.

Simon Edwards
Technical Editor



businesshelp@computershopper.co.uk

Auto pilot Windows Updates and Group Policy

Network administrators can also configure Automatic Updates using the Group Policy Editor. To do this, select Run from the Windows Start menu, type gpedit.msc and press Enter. In the Group Policy Editor, expand Computer Configuration first, followed by Administrative Templates and then Windows Components. Select Windows Update and

double-click on Configure Automatic Updates. In the tab that opens, choose Enabled and then choose the same Automatic Updates settings as you would if you were using the Control Panel.

Users whose Automatic Updates are configured like this will not be able to configure the functions themselves as the options will be greyed out.

stop this, open the Group Policy Editor and navigate to the entry for Windows Updates as above. This time, click on the 'No auto-restart for scheduled Automatic Updates installations' option. Select Enabled and click OK.

THIRD-PARTY UPDATES

Because Windows Automatic Updates transmits information from your PC to Microsoft, the feature is controversial. This is due mostly to a program called Windows Genuine Advantage (WGA). When you try to download software from the Microsoft website, the website uses WGA to check whether your system is running a genuine version of Windows. If the software detects a pirated version, it informs you of this and asks for information on where you bought the software. It also generally refuses to allow you to download the software you wanted.

Automatic Updates is an exception, and WGA still allows you to download important security updates, presumably because the existence of thousands of unpatched PCs would make it easier for malware to spread. Nevertheless, many people feel that what WGA does is an invasion of their privacy. For

this reason, a number of third-party alternatives to Windows Automatic Updates that don't require the use of WGA have been developed.

One of the most popular third-party update programs is Windiz Update, available as a free plug-in for the non-Microsoft browsers Firefox, Netscape, Opera and K-Melon. Once you have installed the plug-in, visit www.windizupdate.com and the site will ask you if you want to scan for updates. It then searches the Windows Update website, just like Automatic Updates, and downloads any fixes your PC needs. Alternatively, you could use Shavlik's NetChk Protect. Shavlik developed a tool for Microsoft called the Microsoft Baseline Security Analyzer (MBSA), which is used by system administrators to determine which updates a networked system requires remotely; see <http://support.microsoft.com> for details.

Shavlik's own product is based on the same technology, but as well as identifying updates for Microsoft products it can also update non-Microsoft products such as the Firefox and Opera web browsers. Last but not least, you could try AutoPatcher (www.autopatcher.com). This free download scours the Microsoft Update website for the downloadable versions of the latest patches; unlike normal updates, these can be installed even when you're not connected to the internet. So not only can you avoid using Windows Automatic Updates, you also accumulate a handy library of updates that can be used to update a newly installed system quickly, even if it isn't connected to the internet.

The downside to using third-party programs is that you have to take the developer's word that the software does not violate your privacy or do anything else that it shouldn't.

OTHER CRUCIAL UPDATES

Windows isn't the only piece of software that needs to be updated regularly. All sorts of

programs are patched regularly by their manufacturers as new features become available or security loopholes are plugged. At least once a week, you should check to see if updates are available for your web browser, Adobe Reader (although this will nag you to check anyway) and, in particular, any security software such as your firewall and anti-virus protection.

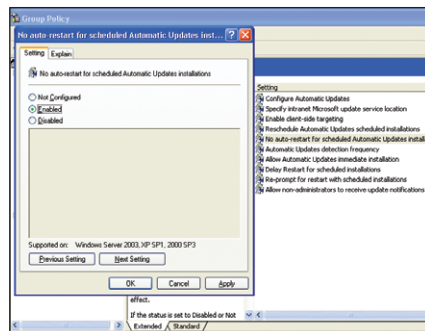
Security programs will almost certainly have an automatic update feature, which you should use. However, before relying blindly on your virus scanner's auto-update feature, find out how often it intends to update. Some products don't update daily, while others do so hourly. You don't want to wait a week without a vital virus definition, although one notable anti-virus program updated itself weekly until recently.

If your security products don't update daily, find out where urgent updates are posted on the manufacturer's website. That way, if there is a huge virus outbreak, you will know where to check. It's also worth making sure your security software is properly configured to use your internet connection. For instance, you may have a proxy server that could interfere with its connection. Will your software warn you if, for some reason, it goes longer than a few days without being able to update itself?

A WORD OF WARNING

You must update Windows and all your security software regularly, or there is a very high chance that your PC will be infected by a virus or other form of malware. However, not all available updates are beneficial.

To write and research this article, we had to remove the Symantec Automatic Update feature and the new Windows search tool, downloaded as part of a batch of updates. Always make regular backups so if an update slows down your PC or breaks a vital piece of software, you can easily go back to the way things were before. **CS**



▲ Stop Windows nagging you to restart after an update

HOW TO... Schedule tasks

Another way of keeping your system safe and running smoothly is to schedule key maintenance tasks to run regularly. Windows has a tool to help you do this called Scheduled Tasks, which is in the Windows Control Panel. To use Scheduled Tasks, your Windows User Account must be protected by a password. One thing to watch out for is that sometimes the program you want to run automatically will start but wait for some interaction before it starts its task. You may have to explore its command-line options to force it to start its job unsupervised.

In the example here, we have used the Windows Disk Cleanup Tool, which can easily be

configured to open and run a specific set of tasks. The basic principles involved work with most programs, though.

1 First you must create a task. From the Start menu, click on Run. In the Run box, enter `cleanmgr /sageset:1`. This opens the Windows Disk Cleanup Tool for the specific purpose of creating a task. In the Disk Cleanup tool, choose the types of file that you would like to delete on a regular basis.

2 From the Control Panel, open Scheduled Tasks and click on Add Scheduled Task.

Next, select the program you wish to schedule – in our case, Windows Disk Cleanup Tool. Decide how often you wish to run the program (we chose weekly), on which day it should run, and at what time. When this is done, finish the Wizard routine.

3 From Scheduled Tasks, open the task you have just created. In the line entitled Run, add a backslash and then the switch that tells that program to run the task you wish to schedule. In our case, this is `sagerun:1`, so the full command line reads `C:\WINDOWS\system32\cleanmgr.exe /sagerun:1`.

